

UNITED STATES DISTRICT COURT

for the
Northern District of TexasIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Google email account gemini908@gmail.com
stored at Google Incorporated, 1600 Amphitheater
Parkway, Mountain View, CA 94043

Case No. 4:16-MJ-

FILED
DEC 27 2016
CLERK, U.S. DISTRICT COURT

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 2252 and 2252A	Possession of Child Pornography

The application is based on these facts:

See Affidavit in Support of Search Warrant

- ☐ Continued on the attached sheet.
- ☒ Delayed notice of 90 days (give exact ending date if more than 30 days: 3-27-17) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Amanda Johnson, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

12/27/16

Judge's signature

City and state: Fort Worth, Texas

Hal R. Ray, Jr., U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I, Amanda Johnson, being duly sworn under oath, do hereby depose and state:

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (HSI), and I have been employed in this capacity since November 2007. I am a graduate of the Criminal Investigator Training Program and the U.S. Immigration and Customs Enforcement Special Agent Training Academy. As a result of my employment with HSI, my duties include, but are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21 and 31 of the United States Code (U.S.C.). I am an “investigative or law enforcement officer of the United States” within the meaning defined in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

2. As part of my duties as an HSI agent, I investigate criminal violations relating to child pornography, including the illegal transportation, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. I have received training in the areas of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in several child pornography investigations and am familiar with the tactics used by individuals who collect and distribute child pornographic material.

3. This affidavit is made in support of an application for a search warrant authorizing the search of the records associated with the email address **gemini908@gmail.com**, stored at the premises owned, maintained and operated by Google, Incorporated, headquartered at 1600 Amphitheatre Parkway, Mountain View, California. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the Government records and other information in its possession pertaining to the subscriber or customer associated with this account, including the contents of communications, which represent evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A.

4. The statements included in this affidavit are based in part on an investigation I have conducted, as well as information provided to me by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me regarding this investigation. I have included only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252 and 2252A is currently stored in the Google records associated with the email accounts **gemini908@gmail.com**, more specifically described in Attachment A incorporated with this affidavit, and **fakespamemail908@gmail.com**.

5. I further submit that the information set forth in this affidavit establishes probable cause to believe that the individual using Google accounts

fakespamemail908@gmail.com and **gemini908@gmail.com** has utilized a cloud-storage account to transport, receive and possess images and videos depicting child pornography. The investigation into this cloud-storage account revealed **fakespamemail908@gmail.com** was provided as the registered email address for the account containing child pornography, and **gemini908@gmail.com** was provided as an alternate communication channel for the individual controlling the account; therefore, the facts and circumstances set forth in this affidavit will show probable cause to believe that these Google accounts will have stored information and communications that are relevant to this investigation, including, but not limited to, the identity of the person controlling the accounts.

DEFINITIONS

6. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and the attachments incorporated herein:

a. “Internet Service Providers” (ISPs) are commercial organizations that provide individuals and businesses with access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet, including telephone based dial-up, satellite-based internet access, dedicated circuitry, or broadband-based access via a digital subscriber line (DSL) or cable television lines. ISPs typically charge a fee, based upon the volume of data, commonly referred to as bandwidth, in addition to the

type of connection that the connection supports. Many ISPs assign each subscriber an account name, such as a user name or screen name, as well as an email address and an email mailbox, and the subscriber typically creates a password for the subscriber account. By using a computer equipped with a telephone (dial-up) or cable modem, the subscriber can establish communication with the ISP, and can access the Internet by means of a combination of the user account name and password.

b. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

c. "Electronic Mail," commonly referred to as e-mail (or email), is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email server, for as long a period of time as it takes to send or receive messages. An Internet email message generally consists of three components: the message envelope, the message header, and the message body; in some cases, it may include a fourth component, an attachment.

Email attachments can include any type of digital file. There are numerous methods of obtaining an email account; some of these include email accounts issued by an employer or an education authority. One of the most common methods of obtaining an email account is through a free web-based email provider such as, MSN, Yahoo, or Gmail. Anyone with access to the Internet can generally obtain a free web-based email account.

d. “Cloud-storage service” refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud-storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop computers, laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit.

e. “Communication channel” means a medium through which a message can be transmitted to its intended audience, such as a print media or electronic media (e.g., oral communications or broadcast). In account subscriptions, it refers to a means of delivering account information to a customer, like email, telephone communication, or facsimile.

f. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, both visually or aurally, and by any means, whether in handmade form (including, but not limited to: writings, drawings,

and paintings), photographic form (including, but not limited to: microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to: phonograph records, printing, or typing), or electrical, electronic, or magnetic form (including, but not limited to: tape recordings, cassettes, compact discs, electronic, or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks or DVD's, Personal Digital Assistants (PDAs), Multimedia Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

INFORMATION REGARDING GOOGLE

7. Google, Incorporated ("Google") is an American multinational technology company specializing in Internet-related services and products. These Internet-related services and products include online advertising technologies, search, cloud computing, and software. Examples of popular Google online services include email (Gmail), cloud-storage service (Google Drive), an office suite (Google Docs), and a social networking service (Google+).

8. Gmail is a webmail service that allows account holders to send, receive, and store emails and attached digital files on Google's servers, or within other Google account service applications. Such emails and digital files can include photographs,

videos, documents, email text, and structured data (i.e., contacts and calendar items).

Google subscribers may obtain email accounts with the “gmail.com” domain name.

9. During the account registration process, Google asks subscribers to provide basic personal information. Based on training and experience in cyber-related investigations, I am aware that Google stores and maintains electronic communications and information about subscribers of their services, including their email service. This information includes account access information, email transaction information, alternate communication channels, and account application information. This information may constitute evidence of the crimes under investigation as it may contain information that will identify the party in control of the subject accounts.

10. Google allows account holders to access their files, which are stored on Google’s servers, from any digital device that can access the Google account application’s website (i.e., Internet accessible devices). I submit that evidence directly relating to the identity of the individual(s) who use a Google account may be found in the information maintained on Google’s servers.

FACTS IN SUPPORT OF PROBABLE CAUSE

11. In March 2016, the New Zealand Department of Internal Affairs (NZDIA) conducted an online investigation into several accounts hosted by Mega Limited (hereinafter, “Mega”), which is a cloud-storage, file-hosting website headquartered in New Zealand. As a result of this investigation, the NZDIA identified a particular Uniform Resource Locator (URL) that contained over 100

files of child-exploitation material.

12. The NZDIA subsequently obtained the contents of the account associated with this URL pursuant to New Zealand law, which included the subscriber and log-in records associated with the account. The records obtained for the account included the following subscriber information:

Account user ID: 10106092550
Registered Email Address: **fakespamemail908@gmail.com**
Account Creation Date: July 3, 2015
IP Addresses: 70.116.154.161; 173.173.90.244

13. NZDIA personnel conducted research into the IP addresses used to create and access this Mega account, and learned both IP addresses are owned by Time Warner Cable and resolve to the Arlington, Texas area. Since the user of this account appeared to reside in the United States, the NZDIA routed the information through Interpol to the HSI Cyber Crimes Center (C3) in Fairfax, Virginia.

14. On or about November 8, 2016, HSI C3 served a subpoena on Time Warner Cable for the subscriber assigned IP address 173.173.90.244 on July 7, 2016, which was the last access date provided in the Mega subscriber records. On or about November 16, 2016, Time Warner Cable complied with the subpoena, and provided the following subscriber information:

Subscriber Name: Steven Bell
Subscriber Address: [redacted], Arlington, Texas
Account Deactivation Date: September 9, 2016

15. On or about November 18, 2016, HSI C3 forwarded this case to HSI Dallas for follow-up, and Special Agent (S/A) Jason Mitchell was assigned the investigation. On or about December 5, 2016, S/A Mitchell obtained a copy of the contents stored in the Mega account under investigation, and observed numerous files that constitute child pornography, as defined in 18 U.S.C. § 2256. The following provides an example of the files that were stored in the Mega account associated with email address **fakespamemail908@gmail.com**:

File Name	Description
10Yo 10Yr Kinderfickervideo Pedoland Papa Vater Fickt (Kinder)-1.avi	A two minute, two second video of a nude prepubescent female child who is bound by the ankles. During the video, an adult male has vaginal and anal intercourse with the child.
000262.mp4	A fifty-four second video of a nude prepubescent male child. During the video, the child inserts an object into his anus while lasciviously displaying his genitals.
0525.mp4	A forty-one second video of a prepubescent male child performing oral sex on an adult male.

Based on my training and experience in child exploitation investigations, I submit that these files constitute child pornography, as defined in 18 U.S.C. § 2256.

16. On or about December 5, 2016, HSI Dallas served a subpoena on Google for the subscriber information relating to **fakespamemail908@gmail.com**. On or about December 15, 2016, Google complied with the subpoena by providing the following subscriber information

for this account:

Name: Spam Spammy
Recovery Email: **gemini908@gmail.com**
SMS: 817-897-2740
IP Addresses¹: 2605:6000:151e:c002:c0a3:7d8d:716:1a08;
192.136.238.7

17. S/A Mitchell researched the IP addresses listed above, which were used to access email account **fakespamemail908@gmail.com**, and determined that both IP addresses are owned by Time Warner Cable and resolve to the Arlington, Texas area. As disclosed in Paragraph 14 of this affidavit, a Time Warner Cable Internet account subscribed to by Steven Bell in Arlington, Texas was used to access the Mega account containing child pornography. At the time of this search warrant application, HSI Dallas is waiting for a subpoena response from Time Warner Cable regarding the subscriber assigned these IP addresses.

18. On or about December 16, 2016, S/A Mitchell researched various open-source and law enforcement databases for intelligence regarding [redacted], Arlington, Texas, which was the address assigned the Internet services used to access the Mega account containing child pornography in July 2016. Records indicate this address is associated with a single-family residence owned and inhabited by the Bell family, whose members include two adult parents and three adult children. To date, the subscriber records obtained from Mega and Google relating to the accounts under investigation do not identify the particular resident

¹ There were several IP addresses provided in the Google records. I have only disclosed the IP addresses relevant to the probable cause in this affidavit.

within this household involved in the transportation and possession of child pornography; therefore, I submit that a search of the contents of email accounts **fakespamemail908@gmail.com** and **gemini908@gmail.com** is necessary to obtain evidence of these offenses, including, but not limited to the identity of the individual responsible for these accounts.

19. Based on my training and experience in child exploitation investigations, I am aware that email is a popular method of Internet communication used by individuals involved in child pornography offenses. I am also aware that it is common for these offenders to provide fictitious subscriber names and contact information during the account registration process, in an effort to disassociate themselves from the account in the event that the email service provider or law enforcement becomes aware of their online activities. I submit that email account **fakespamemail908@gmail.com** is an example of this common occurrence, as the user provided the name "Spam Spammy" during the account registration process.

20. Although individuals who create and utilize fictitious online personas to facilitate child pornography offenses take various steps to maintain their anonymity, I am aware that evidence regarding the true identity of the account user may be found within the contents of the account. This often occurs for several reasons, including but not limited to: 1) these individuals may use the Internet services at their residence or place of employment to access the account;

2) these individuals may use their anonymous email account to receive and/or store messages regarding promotional offers, social media account notifications, or other “spam” communication they do not wish to receive to their primary email account(s)²; and 3) these individuals may provide a legitimate email address or telephone number as an alternate communication channel, in the event that they are locked out of the account and must receive a temporary password or confirmation code to regain access.

21. Based on training and experience, I am aware that it is common for individuals, including, but not limited to those involved in child pornography offenses, to maintain multiple email accounts for different purposes and to send email messages from one personal account to another. When individuals maintain multiple email accounts, they often use similar usernames and passwords (e.g., **fakespamemail908@gmail.com** and **gemini908@gmail.com**) which are only distinguished by a few characters. This is likely done to make it easier for the user to create, maintain, and access the various accounts.

22. Based on my training and experience in child exploitation investigations, I am also aware that individuals who utilize cloud-storage services like Mega to store files depicting child pornography often use email to communicate with other individuals involved in child pornography offenses. These individuals commonly share their child exploitation material by forwarding

² Many times, these messages are addressed to the account user by name, or identify a social media account associated with the user’s true identity.

hyperlinks (and passwords, if needed) to their cloud-storage account to the intended recipient(s) by email. Therefore, I submit that, because **fakespamemail908@gmail.com** is the email account associated with a Mega account used to transport and possess numerous files depicting child pornography, and **gemini908@gmail.com** is the account owner's listed alternate communication channel, the search of these accounts will likely yield significant evidence regarding the transportation and possession of child pornography, including the identity of the offender, and potentially the identification of other individuals involved in child pornography offenses.

CONCLUSION

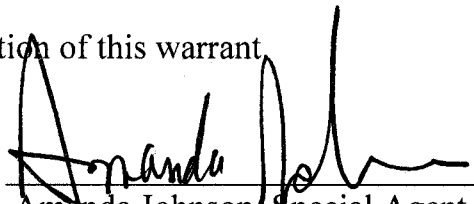
23. Based on the information set forth in this affidavit, I submit there is probable cause to believe that 18 U.S.C. §§ 2252 and 2252A have been violated, and that computer systems under the control of Google, Incorporated contain evidence and instrumentalities of these crimes. Specifically, there is probable cause to believe that email accounts **fakespamemail908@gmail.com** and **gemini908@gmail.com** will contain evidence of these offenses, including, but not limited to, identification of the person who controls these accounts. Accordingly, I request that this Court issue a search warrant requiring Google to produce the records outlined in Attachment A, so that agents may analyze and seize the items outlined in Attachment B.

24. I further request that this Court direct Google to disclose any responsive data by sending it to HSI Dallas, including by use of the U.S. Postal Service or another

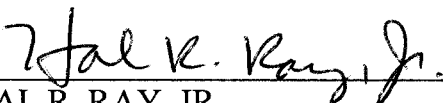
courier service, notwithstanding 18 U.S.C. §§ 2252, 2252A or similar statute.

25. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that - has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(I).

26. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.


Amanda Johnson, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on December 27, 2016.


HAL R. RAY, JR.
UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF TEXAS

**ATTACHMENT A
DESCRIPTION OF ITEMS TO BE SEARCHED**

This warrant applies to information associated with **gemini908@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, Incorporated, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

In order to ensure that agents search only those computer accounts and/or computer files described herein, this search warrant seeks authorization to permit employees of Google, Incorporated (hereafter, "Google") to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts and/or computer files described below, the following procedures have been implemented:

1. The warrant will be presented to Google personnel by law enforcement agents. Google personnel will be directed to isolate those accounts and files described below;
2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files associated with **gemini908@gmail.com**, including an exact duplicate of all information stored in the computer accounts and/or files described below;
3. Google system administrators will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;
4. Google will disclose responsive data by sending to the following recipient using the U.S. Postal Service or another courier service, notwithstanding 18 U.S.C. §§ 2252, 2252A or similar statute or code: Special Agent Jason Mitchell, 125 E. John Carpenter Fwy., Suite 800, Irving, Texas 75062.

5. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the system administrator and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant; and

6. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the system administrator, and will not further review the original duplicate absent an order of the Court.

Section I: Information to be disclosed by Google

To the extent that the information described in Attachment B is within the possession, custody, or control of Google, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs or information that has been deleted but is still available to Google, Google is required to disclose the following information to the Government for each account or identifier associated with **gemini908@gmail.com**:

a. The contents of all emails stored in the account, from the time of account creation to present, including stored or preserved copies of emails sent to and from the account, email attachments, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. The contents of all Instant Messages (IM) associated with the accounts, from the time of account creation to the present, including stored or preserved copies of

IMs sent to and from the account, IM attachments, draft IMs, the source and destination addresses associated with each IM, the date and time at which each IM was sent, and the size and length of each IM;

c. Any deleted emails, including any information described in subparagraph “a” above;

d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

f. All content in the Docs, Calendar, Friend Contacts and Photos areas;

g. Any and all Google IDs listed on the subscriber’s Friends list;

h. All records pertaining to communications between Google, Inc. and any person regarding the account, including contacts with support services and records of actions taken;

Section II: Information to be seized by the Government

All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, messenger logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2)(A), and (a)(5)(B), including, for each account or identifier listed on Attachment A, information pertaining to the following matters, including attempting and conspiring to engage in the following matters:

- a. Any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct;
- b. Any person knowingly transporting, receiving, distributing, or possessing child pornography, as defined at 18 U.S.C. § 2256(8);
2. Credit card and other financial information including but not limited to bills and payment records;
3. Evidence of the identity of the individual(s) who used, owned, or controlled the account or identifier listed on Attachment A;
4. Evidence of the times the account or identifier listed on Attachment A was used;

5. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A and other associated accounts.